Sentinel

Cyber Security: Intro to Cryptography

DEFENDING OUR DIGITAL WAY OF LIFE

Recap

We talked about passwords and authentication as one form of protection

But we also saw that given enough time and effort, most passwords can be cracked

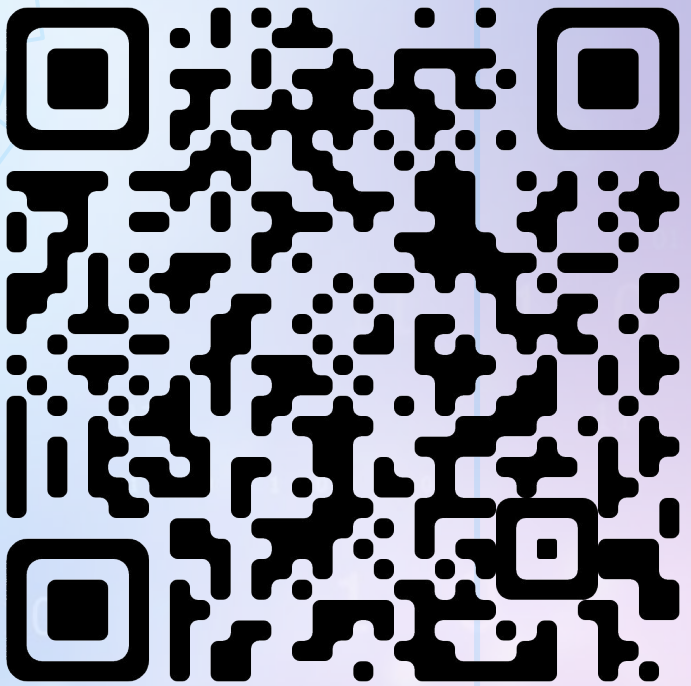
Defense In Depth

In Cybersecurity we'll try to layer many defense mechanisms to safeguard our data

One of the most important layers is **Cryptographically** protecting our data

What is Cryptography?

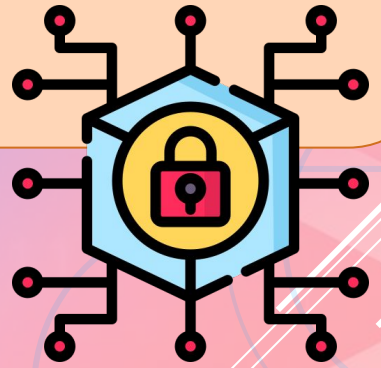
https://youtube.com/clip/UgkxUBtpNrWYRBT6SnUgOF7pfliHWVbjqV6O



Scan the QR code to watch this video!

Cryptography

“the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents”



kryptós, "hidden, secret“
graphein, "writing"

The origins of Cryptography

In ancient times when messages were carried by foot for miles, kings and rulers would encrypt the letters they would send to allies

That way even if the messenger was caught, no one would be able to read or change the message!

What we'll cover this unit

1. Classic cryptographic techniques

2. The advent of cryptographic machines

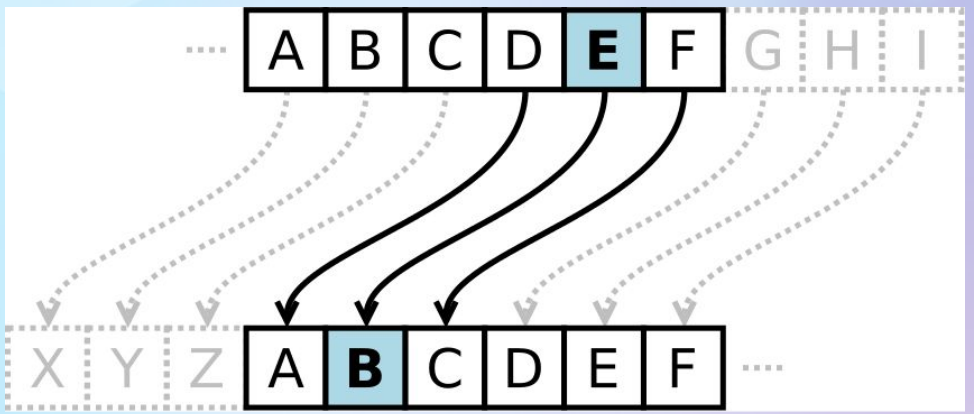
3. The story of the German Enigma Cipher

4. A hint of modern cryptography

Learning Objectives

- What are Substitution Ciphers
- What are Caesar Cipher and Mixed Alphabet Cipher
- How to use patterns in ciphertexts to break ciphers

Caesar Cipher



Shift every letter of the abc.

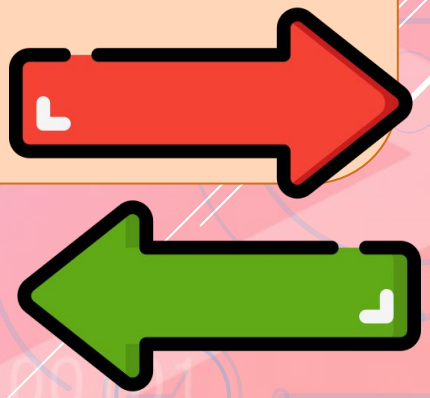
Remember this?

BNWCRWNU VVGGRR QNAN FN PX!

Substitution Ciphers

The **Caesar cipher** is a type of "**substitution cipher**"

"A **cipher** in which each occurrence of a **plaintext** symbol is **replaced** by a corresponding ciphertext symbol to generate **ciphertext**"



Terminology

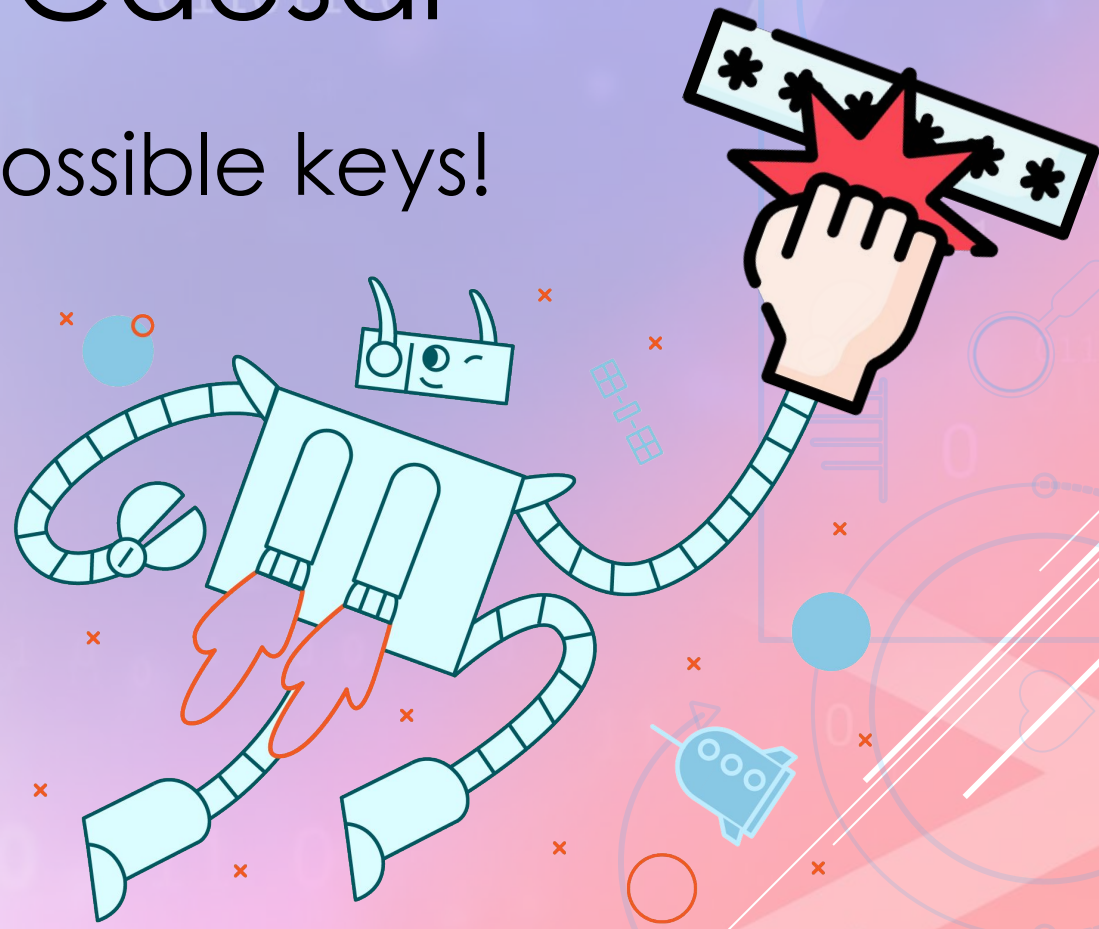
Term	Meaning
Plaintext	Let’s learn crypto!
Ciphertext	Yrg'f yrnea Pelcgb!
Cipher	Rules that convert plaintext into ciphertext

Let’s learn the terms!

Breaking Caesar

Too easy… there are only 26 possible keys!

Brute Force!



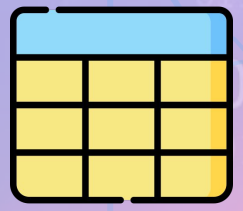
Mixed Alphabet Cipher

Create a **mapping** between each letter and a different letter

A	S
B	U
C	B
D	C
E	I
...	

Worksheet

1. Fill in the **key** table

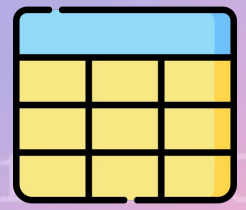


2. Write a plaintext message to encrypt

3. Transform each letter based on the key

Worksheet

Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext Alphabet	K	D	G	F	N	S	L	V	B	W	A	H	E	X	J	M	Q	C	P	Z	R	T	Y	I	U	O



1. Fill in the **key** table

this is my plaintext

2. Write a plaintext message to encrypt

ZVBP BP EU MHKBXZNIZ

3. Transform each letter based on the key

Breaking the cipher

How would you break this cipher?

Brute force?
How many different keys are there to try?

There are 26! (factorial) different possibilities

26! = 403,291,461,126,605,635,584,000,000

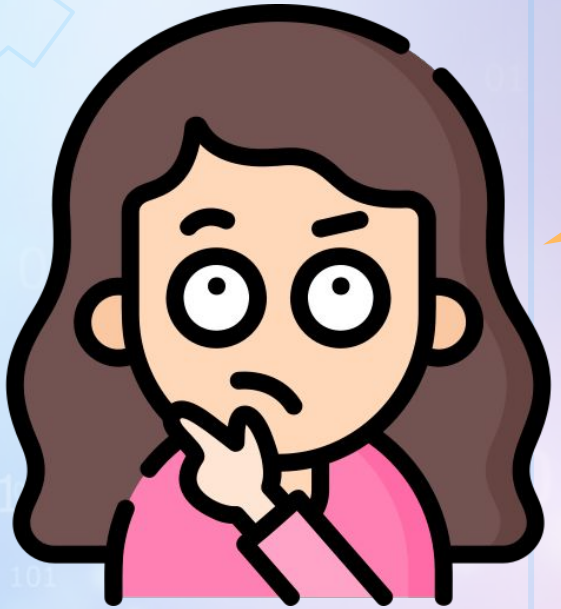
Breaking the cipher

Ok so let's not try to brute force this one 😅

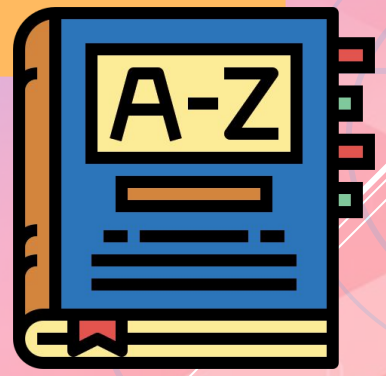
Any other ideas?

Breaking the cipher

We can look at **underlying patterns** in the ciphertext



What types of patterns might English have?



Patterns in English

The most frequent single letter words are: a, I

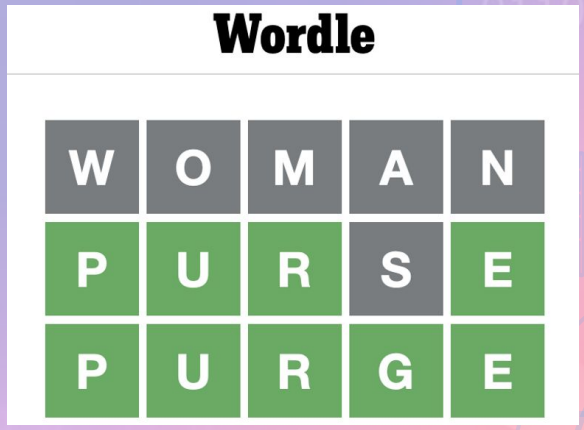
Two letter words are:
of, to, in, it, is, be, as, at, so, we, he, by, or, on, do, if …

Three letter words are:
the, and, for, are, but, not, you, all, any, can, had, her …

Patterns in English

We can also look at letters within words!

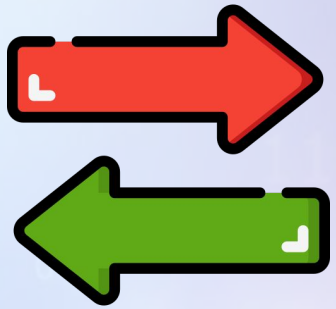
Most frequent letters are:
E T A O I N S H R D L U



The most frequent Digraphs (two letter combinations):
th er on an re he in ed nd ha at en es of or nt ea ti to …

Let's try it out

1. Swap encrypted messages between the pair



2. Take 5 minutes to analyze and try to break the cipher

Do not use online tools (yet)
You can use the cheatsheet (from Moodle)

https://tinyurl.com/cyp-ciphers-ws

Cipher Worksheet (Encrypting)

The mixed alphabet cipher works by replacing every character in the plaintext with a (usually) different character to get the ciphertext. We can create a "key" that tells us how to transform each of the characters of the alphabet:

Plaintext	a	b	c	d	e	f	g	h	i	J	k	L	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	H	N	X	E	L	B	T	J	D	Z	K	R	Q	C	M	A	W	Y	G	S	V	I	O	F	P	U

Using the key table above, decipher the message:

ZHCVH YPNYD CTGSJ LGCMO

Take note, the message is given in blocks of 5 as a convention, and the spaces are not necessarily spaces in the plaintext.

Now it's your turn!

1. Fill up the key table below. Each letter of the plaintext alphabet should be enciphered to one letter of the ciphertext alphabet, and no two letters are enciphered to the same letter.

Plaintext	a	b	c	d	e	f	g	h	i	J	k	L	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext																										

2. Write a short message to your friend in the "Plaintext" box below.

Plaintext:

(Don't let anyone see this!)

3. Transform every character in your message using your key and write it in the "Ciphertext" box on the next page:

Ciphertext:

Now, make a copy of Part B, copy over your ciphertext, and let your friend crack it!

How'd it go?

Troublesome…

Takes a long time

It's hard to break these ciphers by hand

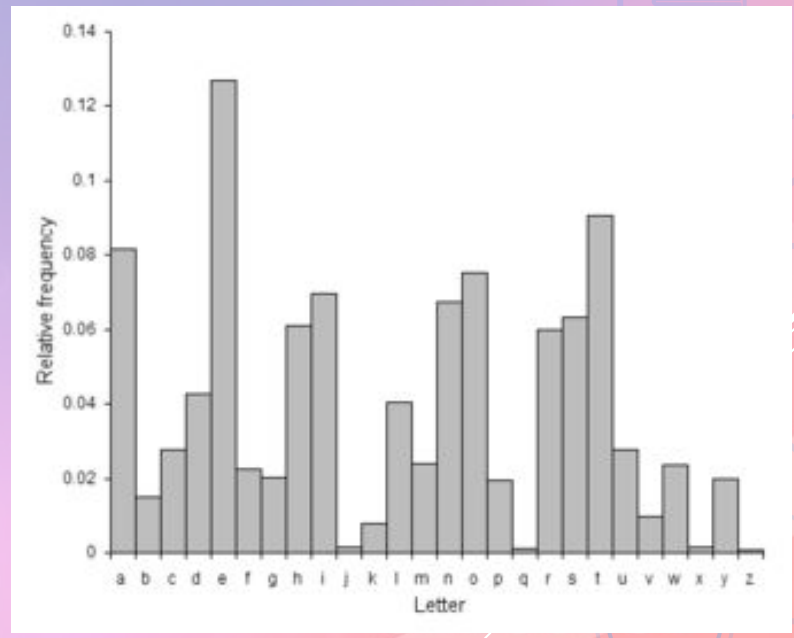
Let's see a tool that can help

Sparking Challenge

Frequency Analysis tool for breaking Substitution Ciphers

Recap

1. Calculate the letter frequencies in the text
2. Compare them to the English text letter frequencies
3. Look for any other patterns (digraphs, words, etc.)
4. Perform substitution until things start to make sense

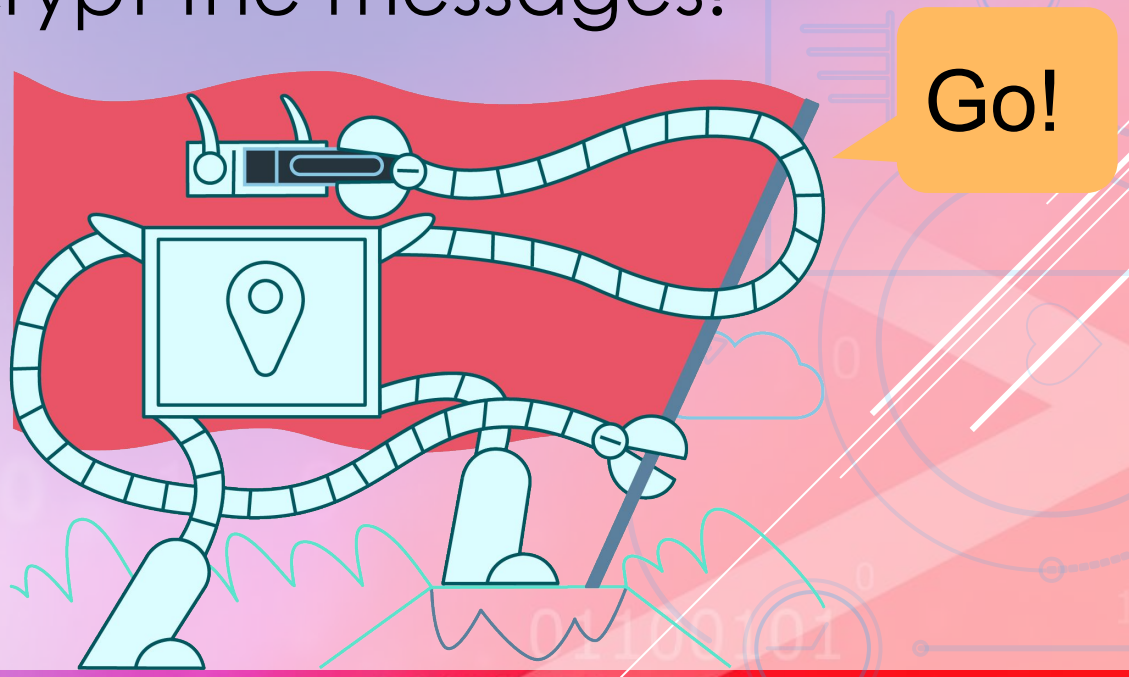


Your turn

Each pair gets ciphertext

Use the analyzer tool to decrypt the messages!

https://sparking-challenge-premium-cypsentinel.replit.app/

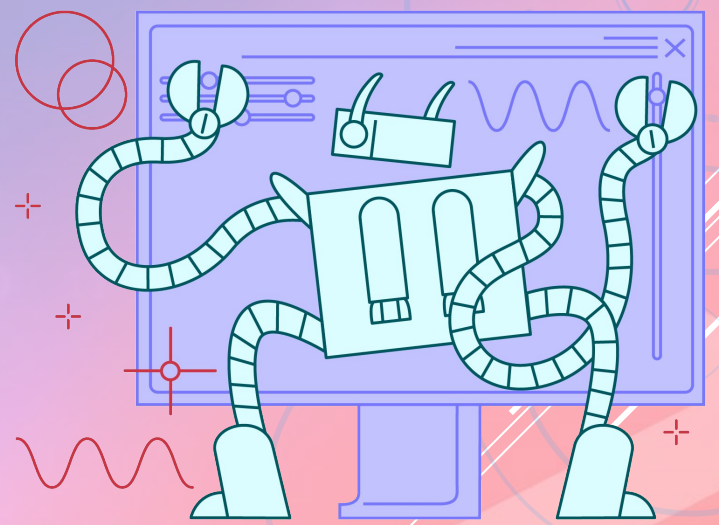


In This Unit You Will

1. Write encryptors/decryptors for a number of different ciphers

2. Break the ciphers!

3. Maybe develop the frequency analysis tool you just used!



Tools of the trade

We'll need to further our programming knowledge:

- String operations
- Functions
- Loops
- Arrays
- Maps
- Advanced DOM manipulation

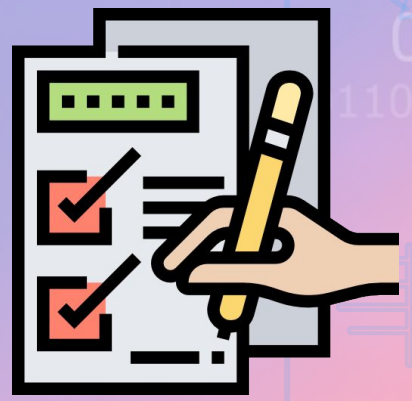
Tools of the trade

These are the basic building blocks of **ALL** apps, everywhere, in any language

At the end of this unit you'll be able to create your own apps from start to finish!

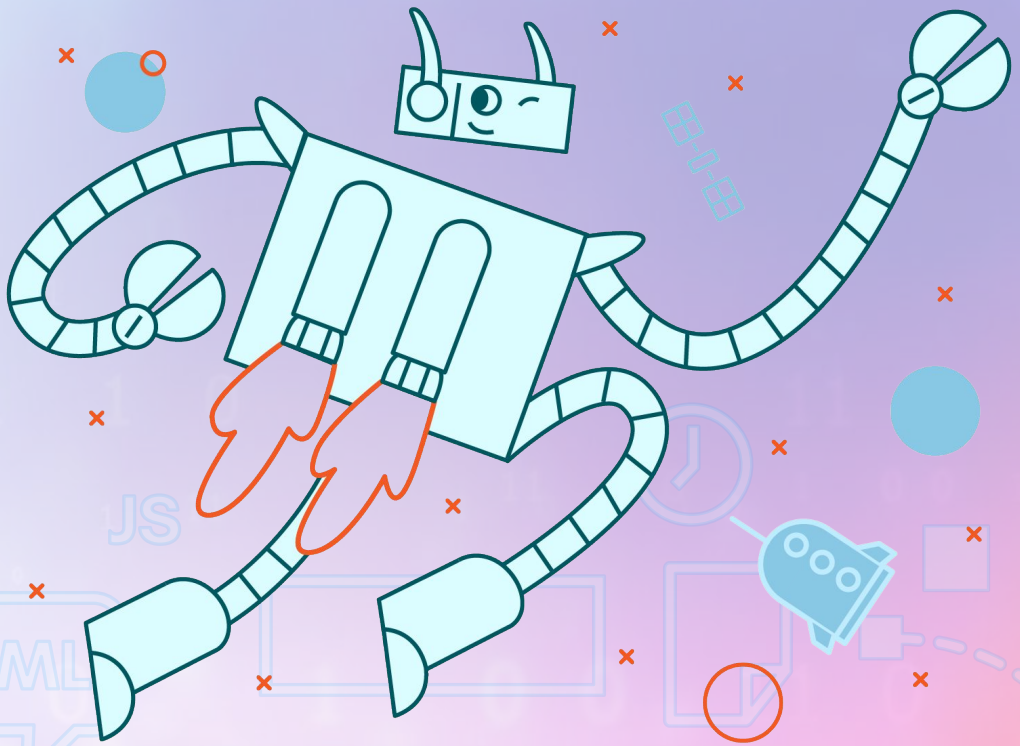
Unit Structure

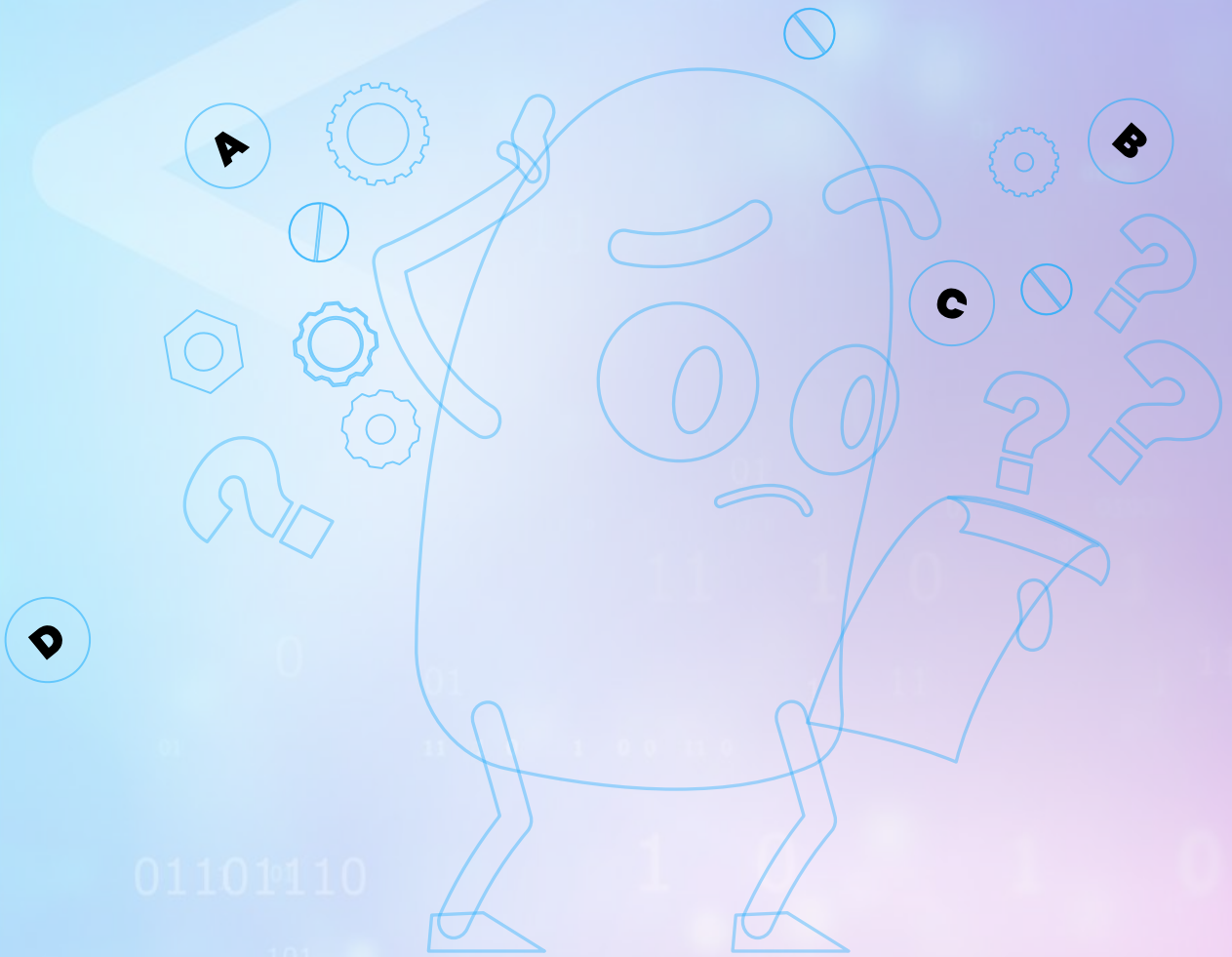
After every new topic you'll have exercise time



Each topic will get us a step closer to achieving our goals!

Let's get to it!





Questions?